



Department of Homeland Security Daily Open Source Infrastructure Report for 29 December 2005

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

Daily Highlights

- The Associated Press reports the timeshare unit of Marriott International Inc. is notifying more than 200,000 people that their personal data are missing after backup computer tapes disappeared from a Florida office. (See item [8](#))
- The Boston Globe reports a 12–inch hole in the fuselage of an Alaska Airlines jet caused the plane to lose cabin pressure, forcing the pilots to make an emergency descent and return to the airport. (See item [11](#))
- The Associated Press reports the New York City health department plans to spend nearly \$1.4 million equipping hospitals with radiation detection devices that might become essential if terrorists detonated a dirty bomb. (See item [28](#))
- US–CERT has released Technical Cyber Security Alert TA05–362A: Microsoft Windows Metafile Handling Buffer Overflow. (See item [37](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES–ISAC) – <http://www.esisac.com>]

December 28, CNN/Money — **U.S. trails in refinery growth according to report.** A surge in oil refinery investment is under way overseas, which could make the United States more reliant on imports of refined products like gasoline and heating oil in coming years, according to a published report. The Wall Street Journal, citing a study by Wood Mackenzie, a consulting firm based in Edinburgh, Scotland, reported that 100 projects representing as much as 12 million barrels per day (bpd) of added refining capacity could be online by the end of the decade, but most of that capacity is outside the United States. U.S. oil companies continue to hold back on building refineries despite the increases seen in 2005 in prices for gasoline, heating oil and jet fuel. While regulatory issues are one barrier, oil companies generally see better returns on investment in oil exploration rather than refinery capacity. While no new refineries are planned, the American Petroleum Institute has said that its members plan increases in capacity at existing refineries equal to one million to 1.3 million barrels of capacity a day in the coming years.

Wood Mackenzie: <http://www.woodmacresearch.com/>

Source: http://money.cnn.com/2005/12/28/news/international/refinery_investments/

2. *December 21, New York Independent System Operator* — **Independent System Operator issues reliability needs assessment.** The New York Independent System Operator (NYISO) Board of Directors recently approved the state's first Reliability Needs Assessment — an important milestone in New York's long-range Comprehensive Reliability Planning Process. The Reliability Needs Assessment (RNA) evaluates generation adequacy and transmission reliability over a 10-year planning horizon, and identifies future needs of the New York electric grid. It is the first step in the NYISO's Comprehensive Reliability Plan, which is a key component of the Comprehensive Reliability Planning Process. "This Reliability Needs Assessment is a blueprint for identifying future needs to maintain the reliable transmission and distribution of power to New Yorkers," said Mark S. Lynch, President and CEO of the NYISO. The NYISO operates the state's bulk power transmission system and administered more than \$10 billion in transactions in the wholesale electric markets in 2005. The RNA process could result in new generation additions and transmission upgrades, as well as stepped-up demand response programs. If market-based solutions are insufficient, the NYISO will request that the appropriate transmission owner proceed with a regulated solution in order to maintain reliability. According to the report, transmission and generation resources should be adequate through 2007.

Comprehensive Reliability Planning Process Reliability Needs Assessment:

http://www.nyiso.com/public/webdocs/newsroom/press_releases/2005/rna_final12212005.pdf

Source: http://www.nyiso.com/public/webdocs/newsroom/press_releases/2005/pr_nyiso_issues_rna_report_122105.pdf

[[Return to top](#)]

Chemical Industry and Hazardous Materials Sector

3. *December 28, Boston Globe (MA)* — **Pipeline break said to cause oil spill in Massachusetts.** A ruptured pipeline at a Broadway oil facility was the source of an oil spill spotted Monday, December 26, in the Chelsea River near Boston, MA, the Coast Guard confirmed. The pipeline, owned by Global Petroleum, allowed 200 to 300 gallons of heating oil into the mouth of the river. An unknown amount also seeped into the soil around the pipeline. The Coast Guard is

investigating the cause of the rupture and an unrelated sheen that appeared on the surface of the nearby Mystic River. Coast Guard officials said Monday that the company was helpful in cleaning up the spill.

Source: http://www.boston.com/news/local/articles/2005/12/28/pipeline_break_said_to_cause_oil_spill/?rss_id=Boston+Globe+---+Today%27s+paper+A+to+Z

4. *December 28, Great Falls Tribune (MT)* — **Cause of seed plant fire in Montana still a mystery.** A fire that destroyed an Anheuser–Busch seed facility in Fairfield, MT, last week was accidental but an exact cause has not been determined, investigators said Tuesday, December 27. The blaze caused between \$500,000 and \$750,000 damage, said Ben Rhodes, Fairfield Volunteer Fire Department Chief. A portion of the highway was closed and some homes were evacuated for more than an hour because of concern about chemicals stored in the facility. The fire did not enter a room that stored the chemicals, according to Teton County Disaster and Emergency Services, but did burn lines used to transfer the chemicals, prompting the evacuation. Workers were not at the plant at the time of the fire, and no one was injured in the blaze. Dave Tweet, regional manager for Anheuser–Busch's seed and elevator operations, said some equipment was destroyed in the fire, but that a full accounting of the damage had not yet been done. He said, "There's a lot of processing equipment in there...I'm sure it's a pretty significant amount of damage."

Source: <http://www.greatfallstribune.com/apps/pbcs.dll/article?AID=/20051228/NEWS01/512280305/1002>

5. *December 27, WTOV 9 (OH)* — **Ammonium nitrate spill in Ohio county.** Tons of hazardous material was spilled at a railroad yard in Carroll County, OH. Officials are investigating how the hazardous material was leaked. Minerva Railroad Yard General Manager Tom Barnett says last week crews from a Pennsylvania company called Industrial Waste Group dumped ammonia nitrate out of train cars that were meant to be cleaned. When handled improperly, the material can be highly explosive. Ammonia nitrate was one of the primary agents used in the Oklahoma City bombing. Carroll County Emergency Management Agency Director Tom Cottis says there's a lot more of the hazardous material in Minerva than was used in the bombing. Officials say an estimated three tons of hazardous material was spilled but there is no threat to people who live in the county.

Source: <http://www.wtov9.com/news/5675461/detail.html>

[[Return to top](#)]

Defense Industrial Base Sector

6. *December 28, Associated Press* — **State Department sanctions foreign companies.** The Bush administration is punishing nine foreign companies for selling missile goods and chemical arms material to Iran. In making the announcement Tuesday, December 27, State Department spokesperson Adam Ereli said the sanctions were based on "credible evidence," which he did not disclose. As a result, Ereli said, the United States will not provide export licenses to the companies for doing business here and will ban U.S. government purchases from the companies. The action was taken under the Iran Nonproliferation Act, which Congress passed in 2000 to deter international support for Iran's nuclear, chemical and biological weapons programs and for missile–delivery systems. The companies named by Ereli are China

Aerotechnology Import Export Corp., the missile exporter China North Industries Corp., Zibo Chemet Equipment Co., the Hongdu Aviation Industry Group, Ounion International Economic and Technical Cooperative Ltd., and the Limmt Metallurgy and Minerals Co., all from China. Two sanctioned Indian companies are Sabero Organics Chemical and Sandhya Organics Chemical. An Austrian firm is Steyr–Mannlicher, which makes assault weapons.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2005/12/27/AR2005122700698.html>

7. *December 28, Government Accountability Office* — **GAO–06–209: Defense Inventory: Army Needs to Strengthen Internal Controls for Items Shipped to Repair Contractors (Report).**

The Government Accountability Office (GAO) has previously reported that the lack of control over inventory shipments increases the Department of Defense's (DoD) vulnerability to undetected loss or theft. GAO evaluated the Army's effectiveness in maintaining accountability of inventory shipped to repair contractors. To conduct its review, GAO analyzed shipment data for fiscal year 2004, surveyed repair contractors that were recipients of inventory shipments, and assessed the Army's adherence to internal control procedures. Inventory shipments included both secondary repair items — components, assemblies, and subassemblies, other than major end items, which may be sent to commercial facilities for repair, alteration, or modification — and government–furnished materiel — assemblies, parts, and other items provided in support of this work. GAO recommends that the Army take actions to strengthen its accountability over secondary repair items and government–furnished materiel shipped to its repair contractors. DoD concurred with six of GAO's recommendations and nonconcurred with one. GAO has deleted this recommendation based on follow–up work by the Army showing that the Army had erroneously provided a duplicate shipment record.

Highlights: <http://www.gao.gov/highlights/d06209high.pdf>

Source: <http://www.gao.gov/new.items/d06209.pdf>

[\[Return to top\]](#)

Banking and Finance Sector

8. *December 28, Associated Press* — **Marriott customer data missing.** The timeshare unit of Marriott International Inc. is notifying more than 200,000 people that their personal data are missing after backup computer tapes went missing from a Florida office. The data relates to 206,000 employees, timeshare owners and timeshare customers of Marriott Vacation Club International, the company said in a statement Tuesday, December 27. The computer tapes were stored in Orlando, where the unit is based. The company did not say when the tapes disappeared. They contained Social Security numbers, bank and credit card numbers, according to letters the company began sending customers on Saturday, December 24.

Source: http://biz.yahoo.com/ap/051228/marriott_missing_data.html?.v=4

9. *December 28, Associated Press* — **Many methamphetamine users turn to identity theft.** Authorities are discovering that more and more desperate users of methamphetamine (meth) are turning to identity theft to pay for their habit, creating a criminal nexus costing Americans millions of dollars. The trend is sweeping the West and spreading to other parts of the country, with one hub of activity in the garages and trailer parks of Riverside and San Bernardino counties on the fringe of suburban Los Angeles. The region was the site of a third of

California's nearly 500 meth lab busts in 2004 and is home to the second-highest number of identity theft victims in the nation. The connection between meth and identity theft is posing a major challenge for authorities, who until recently tended to overlook or neglect identity theft evidence at meth labs in favor of pursuing drug charges that are easier to prove and carry stiffer penalties. U.S. Senator Maria Cantwell (D-WA) has called on the Department of Justice to study the link further and recommend tougher penalties for those convicted of both crimes. Police said meth users known as "cranksters" are drawn to identity theft because they can stay up for days scanning computer records or go "dumpster diving" for discarded financial information.

Source: <http://abcnews.go.com/US/LegalCenter/wireStory?id=1448027>

10. *December 27, Morning Sentinel (IL)* — New laws designed to protect consumer identity.

Beginning January 1, 2006, new legislation aimed at protecting the identity of Illinois consumers will be in effect. The laws, passed during the summer session of the General Assembly, are set out to help those recover quickly from their stolen identities and also better protect individuals' personal information. One law to be implemented the first of the year requires companies to notify Illinois consumers if their personal information is being compromised. This makes Illinois only the second state in the nation to have these set boundaries. Also passed is a law that allows victims of identity theft to freeze their credit reports. This security measure should prevent other thieves from opening additional credit card accounts with the stolen identity's information and also from changing crucial information in the report, including a person's name, birth date, Social Security number and address.

Source: http://www.morningsentinel.com/news/2005/1227/Front_Page/008.html

[\[Return to top\]](#)

Transportation and Border Security Sector

- 11. *December 28, Boston Globe* — Jet with fuselage hole lands in Seattle.** A 12-inch hole in the fuselage of an Alaska Airlines jet caused the plane to lose cabin pressure, forcing the pilots to make an emergency descent and return to the airport, authorities said Tuesday, December 27. The incident Monday, December 26, involved an MD-80 jet en route from Seattle to Burbank, CA. The plane landed safely at Seattle-Tacoma International Airport, and none of the 140 passengers was hurt. A ramp worker acknowledged that he failed to report immediately striking the plane at the gate Monday with a baggage cart or baggage-belt machine, said Jim Struhsaker, a spokesperson for the National Transportation Safety Board. The worker told the agency that although the vehicle touched the plane, he was not aware he had dented it, Struhsaker said. The accident created a crease in the plane's aluminum skin, which opened up into a 12-by-six-inch gash as the jet came climbed to 26,000 feet, Struhsaker said. The crew of Flight 536 reported a loss of cabin pressure about 20 minutes after takeoff, airline spokesperson Caroline Boren said. Oxygen masks deployed for passengers, and the plane made a rapid descent back toward the airport. The worker who damaged the jet was employed by Menzies Aviation, a British company under contract with the airline to provide baggage handling and other ramp services, Boren said.

Source: http://www.boston.com/news/nation/articles/2005/12/28/jet_with_fuselage_hole_lands_in_seattle/

12. *December 28, Washington Post* — **A new emphasis on rail to Dulles Airport.** The effort by the Washington airports authority to speed construction of a rail line across Northern Virginia is a reminder to the region that the railroad's planners intended the train to serve air travelers as well as commuters. Last week, the Metropolitan Washington Airports Authority said it wants to take over the rail program from the Virginia government. That focused new attention on the theory that a Metro station at Virginia's Dulles International Airport could help keep the airport growing at a time when more people want to use the airport but find it harder and harder to deal with the traffic to get there. "When we look at the region, transportation is becoming increasingly more challenging on roadways," said James E. Bennett, president and chief executive of the airports authority, which operates Reagan National and Dulles. Bennett has come to the same conclusion as many others in the airport industry who see rail as a necessary part of the airport of tomorrow.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2005/12/27/AR2005122701068.html>

13. *December 28, USA TODAY* — **Airport security uses talk as tactic.** The Transportation Security Administration plans to train screeners at 40 major airports next year to pick out possible terrorists by engaging travelers in a casual conversation to detect whether a person appears nervous or evasive and needs extra scrutiny. The new security technique, already in use at some airports, adds a psychological dimension to screening by trying to find high-risk passengers based on how they act at checkpoints or boarding gates. Passengers who raise suspicions will undergo extra physical screening and could face police questioning. Airports in New York, Los Angeles, Chicago, Houston, Detroit, and Miami recently began using the technique. Some airport and transit police already look for people acting oddly — such as wearing a heavy coat in the summer or appearing to be doing surveillance — and question them about travel plans. Behavior detection is routine in security-conscious countries such as Israel, where air travelers routinely face aggressive questioning. U.S. Customs officers have long asked arriving travelers questions, often in random order. If a person gives "stumbling answers," that could indicate the person has fraudulent travel documents or plans to overstay a visa, says Customs and Border Protection spokesperson Kelly Klundt.

Source: http://www.usatoday.com/travel/news/2005-12-28-airport-security_x.htm

14. *December 28, New York Times* — **Transit workers in deal to share health plan cost.** The Metropolitan Transportation Authority and the transit workers' union announced a settlement on Tuesday, December 27, in which the authority abandoned its demand for concessions on pensions and the union agreed to have all workers pay a portion of their health insurance premiums. Tuesday night the executive board of the union, Local 100 of the Transport Workers Union, voted to approve the tentative 37-month contract. The city's 33,700 subway and bus workers are expected to vote on the agreement early next month. Bowing to the authority's wishes, the union agreed to a 37-month contract instead of a 36-month contract, making the expiration date January 15, 2009, rather than December 15, 2008. The date change will remove the risk of a paralyzing strike at the peak of the holiday shopping season.

Source: http://www.nytimes.com/2005/12/28/nyregion/nyregionspecial3/28mta.html?hp&ex=1135832400&en=b393ab681b717433&ei=5094&part_ner=homepage

15. *December 28, Associated Press* — **Trucking industry embraces training simulators.** Top-notch simulators have been used by the military, commercial airlines, and public safety

agencies for years, but Schneider National's training program which looks and sounds like a high quality video game but is actually a state-of-the-art training simulator is one of only a small handful of U.S. trucking companies making big bets on the technology. There are a variety of benefits to simulation, trucking executives said, from lowering the cost of training new drivers to improving their skills. And with the industry's employee turnover notoriously high, trucking companies are hopeful simulators can help quickly boost the confidence of young drivers and thereby reduce the percentage of those who quit because of the stress that comes from long stretches behind the wheel. Still, until recently, these advantages were outweighed by the cost of simulators themselves, which could run as high as \$1 million per unit. While much less expensive simulation systems were available as far back as a decade ago, the single-monitor consoles were mainly used for teaching basic shifting techniques, not how to drive on mountain roads or prevent skidding off an icy road. So far, Schneider executives said they like what they see in terms of reduced training costs, fewer accidents, and higher employee retention.

Source: http://www.boston.com/news/local/connecticut/articles/2005/12/28/trucking_industry_embraces_training_simulators/

16. *December 28, Boston Globe* — **Florida route puts Worcester airport back in action.** In its first week of passenger air service in almost three years, the Worcester Regional Airport is posting brisk business, with most of the new Allegiant Air daily round trips to the Sanford-Orlando airport in Florida more than 80 percent full, Massachusetts Port Authority (Massport) officials said on Tuesday, December 27. Despite millions of dollars in Massport subsidies since the 1990s, the Worcester airport has struggled to keep regular service. Allegiant, based in Las Vegas, is the first airline serving Worcester since US Airways Express abandoned the city in February 2003. A November report by Maryland aviation consultants Infrastructure Management Group Inc. said that "existing carriers are unlikely to relocate service" to Worcester, based on poor past experiences for US Airways, American Airlines, and others. Airport officials should focus instead on "new entrant, start-up, and/or charter carriers," such as Allegiant. Worcester is surrounded by airports with frequent service: Logan International Airport in Boston, T.F. Green State Airport outside Providence, RI, Bradley International in Windsor Locks, CT, and Manchester Airport in New Hampshire. But 620,000 people live at least 20 minutes closer by car to the Worcester airport than any of the four others, the report found, offering a key market.

Source: http://www.boston.com/business/articles/2005/12/28/florida_route_puts_airport_in_worcester_back_in_action/

17. *December 27, CNN* — **TSA: Security changes not affecting air-screening times.** Changes allowing some items previously barred from baggage and new security procedures at terminals don't appear to have affected screening times at the nation's largest airports over the holiday travel period, the Transportation Security Administration (TSA) said Tuesday, December 27. The peak wait time for security screening at the nation's 40 largest airports was 13.4 minutes between Thursday, December 22, and Tuesday, December 27, TSA spokesperson Darrin Kayser said. On Thursday, the TSA began allowing some small, sharp, objects in carry-on bags: scissors less than four inches long and tools less than seven inches long. Such items had been prohibited since shortly after the September 11, 2001, attacks in which al Qaeda operatives used knives and box cutters to take over aircraft. In making the change, TSA cited other improvements in security, including the installation of reinforced cockpit doors. The TSA

also began more random secondary screenings of passengers, including enhanced pat-downs, to screen more thoroughly for explosives.

Source: <http://www.cnn.com/2005/TRAVEL/12/27/airport.security/index.html>

[[Return to top](#)]

Postal and Shipping Sector

Nothing to report.

[[Return to top](#)]

Agriculture Sector

18. *December 27, Animal and Plant Health Inspection Service* — U.S. Department of

Agriculture bird biosecurity calendar available. The U.S. Department of Agriculture's (USDA) Animal and Plant Health Inspection Service Tuesday, December 27, announced the availability of a bilingual calendar designed to help bird owners protect their birds from diseases. The free calendar, entitled 2006 Backyard Biosecurity: Keeping Your Poultry Healthy, is an essential tool for bird owners to ensure the prevention of infectious poultry and bird diseases. It provides information on the warning signs for spotting illness and how to report sick birds, as well as six easy-to-follow steps for practicing backyard biosecurity. Biosecurity for the Birds is an important USDA outreach campaign to inform people who raise their own poultry or have exotic birds about the signs associated with diseases. The campaign focuses on common sense biosecurity tips bird owners can take to protect their flocks. There is a great need to take all steps necessary to ensure the continuing economic stability and overall health of the U.S. poultry industry.

Calendar: <http://www.aphis.usda.gov/vs/birdbiosecurity>

Source: <http://www.aphis.usda.gov/newsroom/content/2005/12/calendar.shtml>

19. *December 27, Cincinnati Enquirer (OH)* — Turfway horses to be tested for equine herpes.

Some horses at Kentucky's Turfway Park will undergo another series of tests Wednesday, December 28, after officials euthanized a horse infected with equine herpes Saturday, December 24. Horses in Barn 26 tested positive for being exposed to the virus. None that have the virus showed symptoms, according to track officials. "We have reports that each of those horses appears to be in satisfactory condition with no negative effects resulting from exposure," stated Robert Stout, a Kentucky state veterinarian with the Department of Agriculture. Those horses will be tested again Wednesday, December 28. Officials found no evidence the virus spread outside Barn 26. Park officials announced new requirements to prevent further infections. Beginning Wednesday, December 28, all horses shipping to or from Turfway Park must show health certificates issued within 24 hours. Beginning January 11, all horses providing pony-to-post services or shipping onto the grounds must show proof of inoculation against equine herpes. The inoculation must have occurred within 90 days, but no sooner than January 4.

Equine herpes information: <http://duke.usask.ca/~misra/virology/stud2004/evd/ehv1page.html>

Source: <http://news.enquirer.com/apps/pbcs.dll/article?AID=/20051227/NEWS0103/512270336/1077/rss02>

Food Sector

20. *December 29, Associated Press* — Japan tightens inspections on corn from U.S. Japanese authorities have tightened inspections on corn shipped from the U.S. after finding a poisonous fungus in a shipment arriving in Japan, a government official said Wednesday, December 28. The Health Ministry ordered quarantine offices across Japan on Tuesday, December 27, to tighten inspections after detecting aflatoxin a week ago among U.S. corn unloaded at Yokkaichi port in central Japan, said Yasuki Matsui of the ministry's quarantine station administration. Aflatoxin, a fungus found on corn and other grains, can cause illness in animals and is associated with liver cancer in humans. Matsui said the aflatoxin was found by sample testing among from 200 tons of yellow corn, imported by Sojitsu Corp., a Japanese trading company. Japan has imported a total of 3.76 million tons of corn from the U.S., including 21 tons of sweet corn and 7,613 tons of popcorn, this year through December 20, according to ministry figures. Source: http://mdn.mainichi-msn.co.jp/business/news/20051228p2g00m0b_u013000c.html

21. *December 28, Wall Street Journal* — Major changes set for food labels in 2006. With the arrival of the New Year, a host of additions and changes are in store for food labels. The presence of eight major allergens and the amount of trans fat in a product will have to be disclosed on labels as of January 1. Among the other changes on the horizon, the Food and Drug Administration (FDA), which oversees most food labels, is considering giving calories more prominence on the food label and requiring that nutrition information be spelled out for an entire package, not just for "servings." Also in 2006, the FDA will likely update dietary intake references for nutrients like vitamins to reflect new scientific reports from the National Academy of Sciences. But the transition to more informative labels is likely to bring some confusion, too. The FDA is allowing companies to continue to use labels that were made before 2006 — without allergen declarations. And it has promised to extend deadlines for some companies having difficulty complying with the trans-fat rule. Source: <http://www.post-gazette.com/pg/05362/628974.stm>

22. *December 27, Animal and Plant Health Inspection Service* — Proposal to allow importation of peppers from the Republic of Korea. The U.S. Department of Agriculture's Animal and Plant Health Inspection Service Tuesday, December 27, announced that it is proposing to amend the fruits and vegetables regulations to allow, under certain conditions, the importation of peppers into the continental U.S. from the Republic of Korea. Based on the scientific evidence of a recent pest risk analysis, peppers can be safely imported from the Republic of Korea, provided certain conditions are met, to continue to protect the U.S. against introductions of plant pests and diseases such as *Agrotis segetum*, a moth that feeds on a wide range of host plants, including peppers, and occupies a large climate area. As a condition of entry, the peppers must be grown in approved insect-proof, pest-free greenhouses and packed in pest exclusionary packinghouses. In order to safeguard against pest infestation during their movement, the peppers must be protected by an insect-proof mesh screen or plastic tarpaulin and packed in insect-proof containers. Source: <http://www.aphis.usda.gov/newsroom/content/2005/12/kpeppers.shtml>

Water Sector

23. *December 28, BBC News* — **Fears over Chinese water supply.** The underground water supplies of around 90 percent of China's cities have been polluted by rapid economic growth, a senior environmental official has said. Zhang Lijun, Deputy Director of the State Environmental Protection Administration, called the problem "serious." He said the economy's growth would put enormous pressure on water supplies. China's official media said underground water supplies provide drinking water for nearly 70 percent of China's population and 40 percent of agricultural irrigation. Experts at an environmental hearing in Beijing said rapid economic advances over the past two decades was causing heavy pollution and could lead to an ecological and environmental crisis, the news service reported. Lijun added continued economic growth could see China facing an even more severe situation in the next 25 years. Source: <http://news.bbc.co.uk/2/hi/asia-pacific/4563932.stm>
24. *December 26, Associated Press* — **Wyoming tries cloud seeding to get rain.** Like most other Western states, Wyoming lacks water. So, like other Western states, Wyoming is trying to conjure up rain by embarking on a cloud-seeding project to bolster mountain snowpack — the reservoirs of the arid and semiarid West — and create more water from spring and summer snowmelt. If more snow can be produced in the mountains by cloud seeding, it would mean more water for cities, towns, and farms. But Wyoming's \$8.8 million, five-year cloud-seeding project goes beyond what other states are doing — not only because of its size and scope but also because it could yield definitive proof of whether cloud seeding works. Millions of dollars are already being spent in a number of states, especially in the West, to spew silver iodide into storm clouds to coax more rain and snow to fall. Whether cloud seeding works has been the subject of debate among the scientific community. The Wyoming project seeks to determine whether cloud seeding can increase runoff from three mountain ranges. No cloud seeding is expected to begin until next year. The state is paying \$1.9 million for the National Center for Atmospheric Research to monitor and study the cloud seeding in Wyoming. Source: <http://www.washingtonpost.com/wp-dyn/content/article/2005/12/25/AR2005122500569.html>
25. *December 26, Slidell Sentry–News (LA)* — **Water company pleads guilty to dumping charges.** A Mandeville, LA, based water and sewage company was fined \$2.1 million Wednesday, December 21, after pleading guilty to charges of improperly operating its plants and dumping 46 times the legal limit of waste into local waterways. Southeastern Louisiana Water and Sewage Co, Inc. (SELA), one of St. Tammany's major sewage operators, violated several caveats of the federal Clean Air Water Act at many of its 30 St. Tammany Parish plants during an 11-year period, said Jan Maselli Mann, first assistant U.S. attorney from New Orleans. SELA was charged with operating its facilities without a permit, failing to report violations, and in some cases, falsifying reports, investigators said. Source: <http://www.slidellsentry.com/articles/2005/12/26/news/news02.txt>

Public Health Sector

26. *December 28, Associated Press* — Emergency rooms packed as flu outbreak hits Phoenix.

A flu outbreak is making its way around Arizona and hospitals say their emergency waiting rooms are packed. The emergency room staff at Scottsdale Healthcare Osborn hospital usually sees 100 to 140 patients a day without any wait. On Tuesday, December 27, they saw more than 200 patients and some patients had to wait four hours. State health officials counted 388 reports of flu in Arizona last week — 48 percent of all the cases reported so far this season. Cold weather that passed through Arizona prompted the spike, health officials say. They also say visitors seeking refuge from snow country or staying with family may have brought in viruses. Cases of strep throat, croup, common colds and bronchitis also are showing up, lengthening the line of patients waiting for care.

Source: http://www.cbsnews.com/stories/2005/12/28/ap/health/mainD8EP_62Q80.shtml

27. *December 28, Associated Press* — Bird flu fails to migrate. The H5N1 strain of bird flu appears more likely to wing its way around the globe by plane than by migrating birds. Scientists have been unable to link the spread of the virus to migratory patterns, suggesting that the thousands of wild birds that have died, primarily waterfowl and shore birds, are not primary transmitters of bird flu. Reports this summer and fall of the spread of the H5N1 strain strongly suggested wild birds were carrying the disease outward from Asia as they followed migration patterns that crisscross the Earth. The timing and location of outbreaks in China, Russia, Romania, Turkey, and Croatia seemed to point to wild birds en route to winter grounds. Since the early fall, however, there have been only scattered reports of more outbreaks. The disease has been glaringly absent, for example, from western Europe and the Nile delta, where many presumed it would crop up as migrating birds returned to winter roosts. That suggests the strain has evolved to specifically exploit domestic poultry, whose short lives spent in tight flocks mean a virus has to skip quickly from bird to bird if it is to survive, said Hon Ip, a virologist with the U.S. Geological Survey's National Wildlife Health Center.

Source: http://www.cbsnews.com/stories/2005/12/28/ap/health/mainD8EP_4V886.shtml

28. *December 28, Associated Press* — New York hospitals to get radiation devices. The New York City health department plans to spend nearly \$1.4 million equipping hospitals with radiation detection devices that might become essential if terrorists detonated a "dirty bomb." The equipment, largely paid for with federal grants, could help medical centers diagnose the thousands of people who likely would flood hospitals after such a blast, the department said. The devices would go to public and private hospitals, whose staff members would be trained how to recognize and treat radiation injuries, and how to protect and decontaminate themselves while dealing with patients who may have been exposed. The program, to be implemented in the coming months, is part of a nationwide effort to prepare for possible attacks with nuclear material. Unlike nuclear weapons, which create huge fireballs fed by nuclear chain reactions, dirty bombs would use conventional explosives to scatter radioactive material. That type of blast would not be particularly powerful and would be unlikely to cause many deaths, experts say, but the fear of contamination could spark panic. Tens of thousands of people likely would besiege hospitals, wondering whether they had been contaminated by radiological material.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2005/12/27/AR2005122701335.html>

29. *December 28, Yomiuri Shimbun (Japan)* — **Japanese government to establish conditions for Level 4 bio–safety labs.** The Japanese government will establish within three years conditions for the operation of a bio–safety Level 4 (BSL4) facility that can isolate for safe handling and study dangerous infectious disease agents, a government source said Tuesday, December 27. The handling of the most dangerous agents has been suspended at the two existing BSL4 facilities in the country because of the opposition of local residents. The Council for Science and Technology Policy decided Tuesday, December 27, to consider setting up another BSL4 facility if the two existing facilities are found not to meet necessary conditions the government will set in the future. The government aims to start operating a functional BSL4 facility as soon as possible. The decision is expected to enhance the nation's ability to handle infectious diseases as the international community is increasingly on alert against bioterrorism. Currently, agents that cause highly dangerous infectious diseases, such as the Ebola virus, cannot be handled domestically because of the suspension at the two domestic BSL4 facilities, making it impossible for Japan to diagnose such diseases and develop medicines or vaccines against them. Even if a person is suspected to be infected with such a virus, it would be impossible to examine his blood for contamination.
Source: http://www.yomiuri.co.jp/dy/features/science/20051228TDY0100_5.htm

30. *December 23, Oregon State University* — **Pharmacist–delivered vaccinations boost vaccination rates.** A new study shows that retail pharmacists' efforts to provide vaccinations to the public—at–large is a growing success and will likely have wide–ranging impact on vaccination rates for a number of diseases. Study authors David Bearden and Tom Holt's analysis of pharmacist–delivered vaccinations is the first statewide report of a voluntary pharmacist–delivered vaccination program in community pharmacies. Oregon first granted authority for retail community pharmacists to vaccinate patients in 2000. Tracing pharmacist–delivered influenza vaccinations in Oregon for the first three years of the program, the research shows that pharmacists provided a substantial number of flu shots, with rural counties accounting for 28 percent of the vaccinations. Pharmacist–provided vaccinations offer a unique opportunity for states with large rural areas to reach rural populations, Bearden said. Data shows that pharmacies are well–accepted as vaccination sites and provide an easy option for any patients who otherwise might not receive a vaccination. Bearden and Holt found that 56 Oregon pharmacies provided immunizations during the first year of the program. In the second year, the number increased to 88, and by the third year of the study, 132 pharmacies, or 18.4 percent of the licensed retail drug outlets in Oregon, were participating.
Source: <http://oregonstate.edu/dept/ncs/newsarch/2005/Dec05/fluvacci nes.htm>

[[Return to top](#)]

Government Sector

31. *December 28, Associated Press* — **White County judges: Courthouse unsafe.** Judges and law enforcement officials in Georgia's White County say the existing courthouse in Cleveland is unsafe and needs to be improved immediately. Sheriff Neal Walden said, "In almost any rural courthouse, you can walk through three of four different entrances. That's just the way they were designed. But times have changed. You've seen what happened in Fulton County." Brian Nichols is accused of killing Superior Court Judge Rowland W. Barnes, a court reporter and a deputy during a shooting rampage in the courthouse in Atlanta, Fulton County, last March 11.

Walden said there are no deputies stationed at the courthouse on days when court is not in session. He has asked the county commission for two additional officers, who would be assigned fulltime to the courthouse. Walden also has recommended rekeying the courthouse doors, restricting public access to just one entrance, and purchasing a metal detector.

Source: http://www.11alive.com/news/news_article.aspx?storyid=73848

[[Return to top](#)]

Emergency Services Sector

32. *December 28, Rochester Democrat and Chronicle (NY)* — **Constellation Energy discusses emergency plan.** Constellation Energy officials gave a short media presentation Wednesday, December 28, and have mailed informational calendars about their response plan in the event Ginna Nuclear Power Plant has an emergency. Officials spoke at a coffee shop about the emergency response planning procedures and talked about the calendars that were given to the 58,000 residents living within a 10-mile radius of the plant. The calendar includes information about Ginna's siren systems, where residents will hear a steady signal for about three to five minutes if an accident occurs. Also included is information about radiation, evacuation routes and maps, emergency response planning area and a glossary of essential terms. Even though the plant has safeguards to prevent accidents and material from being released in the area, officials said an educated public could help alleviate the stress of the situation. Peter Polfleit, emergency planner for the company, said there are emergency bus pick-up points and that people should listen to the radio before panicking.

Source: <http://www.rochesterdandc.com/apps/pbcs.dll/article?AID=/20051228/NEWS01/512290301/1007/SPORTS>

33. *December 28, North Kitsap Herald (WA)* — **Washington school district prepared for emergencies.** In the event of a major problem, the North Kitsap School District (NKSD) in Washington state is prepared. Every current teacher is required to take at least one training course either with the Kitsap County Department of Emergency Management or with a facilitator, said NKSD emergency coordinator Jim Noeldner. NKSD's emergency management system relies on emergency response teams. Staff is divided up into eight teams, each with a different focus of response. Incident management, damage assessment, evacuation, disaster first aid, search and rescue, fire and utilities, student/parent reunion, student/staff supervision and site security and food support teams are in place throughout the district with the roles of each defined in the schools' emergency preparedness plans. Each year, each school in the district is required to rehearse what to do in the event of an emergency. Each school in the district has its own barrel of supplies that could be used in the event of a shut-in or natural disaster. From generators, flashlights, food and water, foreseen necessary supplies are in place.

Source: <http://www.northkitsapherald.com/portals-code/list.cgi?paper=95&cat=23&id=562067&more=>

[[Return to top](#)]

Information Technology and Telecommunications Sector

34. *December 28, SC Magazine* — Instant messaging threats to increase next year.

MessageLabs warned that malicious users will increasingly target instant messaging (IM) in the next year, calling it a "widening backdoor" to infect enterprises with spam and trojan attacks. In a year-end report, the company said, "Spammers will diversify further into the IM ecosystems, as business adoption of IM increases and as the 'big three' IM protocols begin to standardize in 2006 and onwards." The report also noted a considerable increase in phishing emails sent this year, representing 13 percent of malicious emails intercepted during 2005, with a high of 27 percent in January. In total, more than 62.5 million phishing emails were intercepted by MessageLabs since Saturday, January 1, an increase of 238 percent from the 18 million caught the year before. The company also predicted more attacks on mobile devices: "Criminals will continue to attempt to gain access to users' mobile devices as the proliferation of wireless technologies like Wi-Fi spreads to airplanes, trains, and other public locations." Analysts found targeted attacks on specific industries became more common in 2005. Over all, MessageLabs reported one in every 36.15 emails sent this year contained a virus or Trojan. The report noted that cybercriminals chose more specific targets during 2005.

Source: <http://www.scmagazine.com/uk/news/article/533780/firm-im-threats-increase-next-year/>

35. *December 28, BBC News* — Criminals target viruses for cash. At first glance, 2005 looks like it was a quiet year for computer security because there were far fewer serious Windows virus outbreaks than in 2004. According to figures gathered by security firm Symantec, there were 33 serious outbreaks in 2004. In 2005, there were only six such incidents. "We're talking about a substantial decrease in worldwide pandemics," said Kevin Hogan, senior manager in Symantec's security response team. This decline is taking place because virus makers have largely stopped spreading their malicious wares with mass-mailers that try to infect as many people as possible via their inbox. Instead, virus creators are cranking out more versions of malicious programs than ever before. Year-end statistics from Finnish anti-virus firm F-Secure show that there were 50 percent fewer virus outbreaks in 2005 but the number of malicious programs has grown by, on average, 40 percent for the last two years. Similarly Sophos reported that it found 1,940 new malicious programs in November 2005, the largest increase since records began. Security experts say this explosion in variants is partly driven by a desire to overwhelm anti-virus firms.

Source: <http://news.bbc.co.uk/2/hi/technology/4521844.stm>

36. *December 28, Security Focus* — Microsoft Windows Graphics Rendering Engine WMF format unspecified code execution vulnerability. Microsoft Windows WMF graphics rendering engine is affected by a remote code execution vulnerability. The problem presents itself when a user views a malicious WMF formatted file, triggering the vulnerability when the engine attempts to parse the file. The issue may be exploited remotely or by a local attacker. Any code execution that occurs will be with SYSTEM privileges due to the nature of the affected engine. Microsoft Windows XP is considered to be vulnerable at the moment. It is likely that other Windows operating systems are affected as well. Security Focus is not aware of any vendor-supplied patches for this issue.

Source: <http://www.securityfocus.com/bid/16074/discuss>

37. *December 28, US-CERT* — Technical Cyber Security Alert TA05-362A: Microsoft Windows Metafile Handling Buffer Overflow. Microsoft Windows Metafiles are image files

that can contain both vector and bitmap-based picture information. Microsoft Windows contains routines for displaying various Windows Metafile formats. However, a lack of input validation in one of these routines may allow a buffer overflow to occur, and in turn may allow remote arbitrary code execution. This new vulnerability may be similar to one Microsoft released patches for in Microsoft Security Bulletin MS05-053. However, publicly available exploit code is known to affect systems updated with the MS05-053 patches. Not all anti-virus software products are currently able to detect all known variants of exploits for this vulnerability. However, US-CERT recommends updating anti-virus signatures as frequently as practical to provide maximum protection as new variants appear. There is no known patch for this issue at this time. Information on potential workarounds is available on the US-CERT Website.

Microsoft Security Bulletin MS05-053:

<http://www.microsoft.com/technet/security/Bulletin/MS05-053.msp>

US-CERT Vulnerability Note VU#181038, Microsoft Windows Metafile handler buffer overflow: <http://www.kb.cert.org/vuls/id/181038>

CVE-2005-4560: <http://nvd.nist.gov/nvd.cfm?cvename=CVE-2005-4560>

Source: <http://www.us-cert.gov/cas/techalerts/TA05-362A.html>

38. *December 27, Security Focus* — **Microsoft Internet Explorer HTML parsing denial of service vulnerabilities.** Microsoft Internet Explorer is affected by multiple denial of service vulnerabilities. An attacker may exploit these issues by enticing a user to visit a malicious site resulting in a denial of service condition in the application. Security Focus is not aware of any vendor-supplied patches for this issue.

Source: <http://www.securityfocus.com/bid/16070/discuss>

39. *December 27, Security Tracker* — **Bugzilla 'syncshadowdb' unsafe temporary files may let local users gain elevated privileges.** A vulnerability was reported in Bugzilla in the 'syncshadowdb' script wherein a local user can obtain elevated privileges. The 'syncshadowdb' script uses temporary files in an unsafe manner. A local user can create a symbolic link (symlink) from a critical file on the system to a temporary file to be used by the script. Then, when the script is executed by the bug tracking system, the symlinked file will be created or overwritten with the privileges of the bug tracking system. The vulnerability can enable a local user to obtain the privileges of the bug tracking system. The vulnerability affects Version(s): 2.6.10 and prior versions. Versions 2.18.* and 2.20.* are not affected. Security Tracker reports that the fix will be included in the pending 2.16.11 version but a solution is currently available.

Solution: https://bugzilla.mozilla.org/show_bug.cgi?id=305353

Source: <http://www.securitytracker.com/alerts/2005/Dec/1015411.html>

Internet Alert Dashboard

DHS/US-CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US–CERT Operations Center Synopsis: US–CERT is aware of a third party report of multiple heap buffer overflows in the Symantec RAR decompression library (Dec2RAR.dll). Although there is limited information concerning this reported vulnerability, US–CERT encourages users and system administrators to consider filtering or disabling the scanning of RAR archives at email or proxy gateways. However, disabling RAR scanning may compromise the effectiveness of the security product. In addition, blocking RAR archives may prevent legitimate information from entering the network. By using a specially crafted RAR archive, a remote attacker may be able to perform any of the following malicious activities:

Execute arbitrary code, possibly SYSTEM privileges

Cause a denial of service condition, possibly disabling antivirus capabilities

Take complete control of a vulnerable system

More information can be found in US–CERT Vulnerability Note VU#305272, Symantec RAR decompression library contains multiple heap overflows, at URL: <http://www.kb.cert.org/vuls/id/305272>

Current Port Attacks

Top 10 Target Ports	1026 (win-rpc), 80 (www), 25 (smtp), 27015 (halflife), 445 (microsoft-ds), 4142 (oidocsvc), 53 (domain), 135 (epmap), 139 (netbios-ssn), 113 (auth) Source: http://isc.incidents.org/top10.html ; Internet Storm Center
----------------------------	--

To report cyber infrastructure incidents or to request information, please contact US–CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[[Return to top](#)]

Commercial Facilities/Real Estate, Monument & Icons Sector

40. *December 28, Associated Press* — Man killed in California mall shooting. A man was killed when an argument at a busy shopping mall in Bakersfield, CA, erupted into gunfire Tuesday, December 27, police said. The Valley Plaza Mall was packed with post-holiday shoppers when the shooting began, sending people screaming and running out of the building, witnesses said. The 20-year-old victim was shot at least once in the chest in front of a sporting goods store, Bakersfield police Lt. Joe Bianco said. Authorities said they believe the shooting was gang-related. Mall surveillance video showed the victim arguing with a group of young men shortly before the shooting.

Source: <http://www.newsday.com/news/nationworld/nation/wire/sns-ap-mall-shooting.0.5445786.story?coll=sns-ap-nation-headlines>

41. *December 28, Towson Times (MD)* — Towson Town Center mall scene of robbery. Baltimore County police are looking for two men who robbed a Fallston man in a Towson Town Center bathroom last week. The men were caught on the mall's new video surveillance

system, which was installed in October after a shooting death there. Thomas Schevrich was in the first-floor bathroom of the mall shortly before 3 p.m. December 21 when two men attacked him, according to Bill Toohey, a police spokesperson. This is the fifth unarmed robbery at the mall in the past 12 months, according to Toohey. "About eight million people, the population of New York City, go through the mall every year," Toohey said. In February, William Bassett was shot to death during a robbery attempt in a parking garage at the mall. His death resulted in a county law requiring some shopping centers to continuously monitor at least 75 percent of their parking lots. In October, the Towson Town Center publicly unveiled its state-of-the-art video monitoring system, which according to mall officials cost well over \$1 million. About 200 cameras monitor much of the one-million-square-foot mall, including its parking garages. Charles Crerand, mall general manager, said at the time that the system, which feeds images to a bank of 16 monitors, exceeds county law requirements.

Source: http://news.mywebpal.com/news_tool_v2.cfm?pnplID=659&NewsID=684904&CategoryID=1840&show=localnews&om=1

[[Return to top](#)]

General Sector

42. *December 28, CNN* — **Fires kill at least four in Texas.** No immediate end appears in sight to the dry conditions fueling fires in tinder-dry Texas and in Oklahoma. Firefighters were battling swift-moving blazes in Texas, where four people were killed on Wednesday, December 28. The fires have charred more than 13,000 acres in central, north-central and northeast Texas. "There is little or no chance of rain for the next several days," said Jack Colley, the chief of Texas Emergency Management Division, in a report about the fires. "The problematic weather condition of high winds and low relative humidity levels forecast ... will produce extreme fire danger over most of the state," he said. More than 100 buildings, including 78 homes, were destroyed Tuesday, said Colley. One of the most endangered areas is in Callahan County, about 125 miles west of Dallas, where a fire that started just outside the town of Cross Plains swept through homes and buildings. Texas Governor Rick Perry declared a disaster Tuesday, December 27, dispatching National Guard troops to battle the flames. In Oklahoma, authorities were reporting fires that have charred thousands of acres across 12 counties. No deaths have been reported in the state. A statewide burn ban is in effect.

Source: <http://www.cnn.com/2005/US/12/28/txok.fires/>

[[Return to top](#)]

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:

<http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.